Journal of Intelligent Systems and Internet of Things (JISIoT)
Vol. 09, No. 01, PP. 84-96, 2023
DOI: https://doi.org/10.54216/JISIoT.090106

A Novel Approach for Enhance Fusion-based Health-care System in Cloud Computing

S. Phani Praveen[1*], Balamuralikrishna Thati[2], Ch Anuradha[3], S. Sindhura[4], Mohammed Altaee[5], M. Abdul Jalil[6]

[1]Department of CSE, PVP Siddhartha Institute of Technology, Vijayawada, India, [2]Department of CSE, Dhanekula Institute of Engineering and Technology, Vijayawada, Andhra Pradesh, India, [3]Department of CSE, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India, [4]Department of CSE, NRI Institute of Technology, Agiripalli, Andhra Pradesh, India, [5]Department of Medical Instruments Engineering Techniques, Alfarahidi University, Baghdad, Iraq, [6]Department of Computer Engineering Techniques, Alturath University College, Baghdad, Iraq
Emails: sppraveen@pvpsiddhartha.ac.in; balu.thati9@gmail.com; akshayagokul2009@mail.com; ssindhurapraveen@gmail.com; m.altaee@alfarahidiuc.edu.iq; mohammed.jalil@turath.edu.iq

Abstract

Individual's start-ups and large corporations in the health-care sector have new opportunities to outsource data and outsourcing computation offers to cloud computing. Although the cloud computing paradigm presents users with interesting and cost-effective opportunities still in its early stage, and using the cloud introduces with new obstacles. An another issue is the security of cloud data, which may be affected the data particularly in the case of health-care systems that store and process sensitive data and is outsourced to a cloud computing system. Although there has been significant progress in the development of health services, there are still issues that need to be settled regarding, integrity, the security, large-scale deployment, service integration, and confidentiality of sensitive medical data. To ensure that sensitive medical data is captured, stored, and consumed securely, an information sharing policy syntax based on rules, the data capture and auto identification reference platform features a Single Point of Contact as well as data buckets that are hosted on a cost-effective cloud infrastructure and scalable. As a result, security, accuracy, and precision are achieved in this analysis and query time is reduced.

Received: January 27, 2023 Revised: April 17, 2023 Accepted: June 11, 2023

Keywords: Data Security; Cloud Computing; Dynamic Cloud Computing Architecture; Data Privacy; Auto Identification Reference; Data Capture

1. Introduction

In the field of cloud computing, multiple disciplines have access to a new technology that allows them to create a virtual department of IT over the Internet [8]. Similar to traditional IT departments, cloud computing provides a variety of virtual services such as storage, stream data centers, and database servers. Pay-per-use business models enable individuals and businesses in the health-care sector to provide cloud services for a minimal cost. An eHealth system faces several issues with cloud computing.

Benefits of managing electronic health records (EHRs) include easy access and use of patient data as well as no limitations on time, space, or human resources for patient monitoring. Health-care organizations have been using the Internet for general health information sharing over the past 10 years which has managed to help patients to understand their conditions. Data communication and electronic information security require additional security measures.

Information security and privacy in the health-care industry are becoming more and more crucial as a result of technological advancements. The sector's increasing dependence on computer-based systems has made them more open to attack from malicious actors. Quality of service (QoS) measures must be developed to ensure secure EHR storage and access management. Patient data can be electronically stored in a variety of places, including locally on a computer, remotely on a corporate network, and on specific storage servers using cloud computing. Maintaining a healthy balance between security and resource access speed while taking into consideration that security requirements are increasing as IT systems become more difficult to utilize is complex.

Unpatched applications, computer viruses, malicious code, and malicious software routines can disrupt routine operations of health-care information systems resulting in damage to EHR. Software updates, firewalls, and antivirus applications are just a few of the necessities for protecting an information system. Because protected access contains confidential medical information, the EHR needs to be secured so that only authorized personnel can access and use it. Protecting EHRs, databases, and medical applications through multi-factor authentication is the only way to guarantee the protection of data against unauthorized access. A large part of the content in the EHR is referred to as "sensitive" data, which is frequently associated with confidential information, so the IT departments working on healthcare should be aware of the latest laws and challenges related to security and privacy. There is a growing trend of standardizing information from medical terminology to networking protocols as soon as possible, since they make it possible to store medical records electronically and send them anywhere in the world, instantly access it. Promoting and maintaining the fundamental medical ethical principles and social expectations that must be met to promote requires a combination of human resources and security technology to protect health information from online criminal activity.

However, it will be going to be difficult for the eHealth sector to adopt cloud computing. Mainly because it is difficult to entrust an external system with sensitive data. When trying to discuss sensitive data, it is important to recognize that our health information is the most private and personal, we have making it the most important and valuable data we have ever had. Therefore, the highest priority is to create dependable eHealth services with security features similar to those discovered in commercial bank.

One of the biggest challenges users face is the migration of data and applications between cloud computing systems or from one cloud computing system to another. Data security issues are just one of the side effects of migration that could occur. When a regular application is transferred to a cloud computing system requiring the (API) security functions to be redefined or modified to use the cloud and a user may encounter difficulties. Each cloud computing system provides its own set of services.

The security of a network refers to the secure transmission of data between two authorized users, while the security of data refers to only authorized users having access to data. Data stored in the cloud are subject to network and data security problems because the Internet is a crucial part of its infrastructure.

Public cloud vendors are untrusted cloud vendors, so customers must send their data to them. In addition to network and data hacking problems users who share their data with cloud vendors risk having their privacy violated by other users harmful programs or even the cloud vendor. Outsourcing data to the cloud can lead to data privacy issues. Encrypted data prevent original data from being provided to cloud vendors. For some like mobile devices encryption for every unique piece of original data is neither feasible nor cost-effective. For instance, some mobile devices utilized in eHealth systems have constrained central processing unit (CPU), RAM, and battery life.

By defining template-as-a-service (TaaS) a cloud vendor can standardize their cloud services. This architecture adds a new layer to cloud computing systems. Cloud vendors can define a standard and generic cloud service based on front-end TaaS (FTaaS) by defining the FTaaS and back-end (BTaaS) sections of TaaS. In other words by offering a consistent interface at FTaaS that enables various cloud vendors to standardize their services DCCSOA assists users in sending their data and applications between cloud vendors.

Both the ubiquitous provision of healthcare and the utilization of modern communication infrastructures in healthcare are commonly referred to as eHealth. It is necessary to reform and digitalize the entire health-care system including its supply, management, and production processes. Such technological innovations are expected to improve the level of quality of healthcare services while rapidly reducing operating and capital expenditure. The governments of the United States, Canada, the United Kingdom, Japan, Korea, and the European Union are keen to change the way, their traditional health-care services are provided and to give eHealth top priority on their policy agendas as a result.

These services must be incorporated into adaptable, reliable, cost-effective, and multifunctional systems, which

consider for an open eHealth services platform. eHealth systems as well as defined as the application and delivery despite the fact that individual eHealth services have received a large amount of research attention. Another significant challenge in eHealth is using the patient data that has been captured while maintaining strict user access in various contexts and forms. Inconsistency and data loss have serious resulted because health-care data are subject sensitive to a variety of threats and attacks [10]. A complete eHealth services platform should also include tools for preserving sensitive medical data's security, auditability, confidentiality, and integrity over the course of their lifetime.

Early on in its evolution the fundamental concept of eHealth was to modernize existing medical systems by digitizing existing personal health records. The conversion of paper records to digital ones demonstrated the value and advantages of the overall project and had a significant effect on the health-care industry. As a result, researchers concentrated on finding new and improved ways to design and deliver health-care services that go beyond data digitization to advance their field of study. Scientists developed these concepts in eHealth platforms, particularly allowing patients to access their personal records anywhere and electronically share their medical summaries. Furthermore, researchers working on the eHealth component are utilizing technologies like smart phones to develop services that let patients gather daily data and learn more about good behaviors.

With the advancement of technologies such as mobile phones and fast internet, eHealth has become widespread due to its positive effects on the daily health experiences of millions of people. The rise of cloud computing created the conditions for an even larger evolution as the eHealth sector began to follow and adopt new technologies and developments in related fields. eHealth development and adoption globally could be significantly accelerated by combining cloud computing and eHealth. This is because cloud services can be flexible. specifically, cloud computing can help in the development of more dependable medical services that will provide us with the functionality we need to better manage our health and maximize the accuracy of our care services.

There has been extensive research on the value of creating safe eHealth services and the benefits of cloud computing and moving current health-care systems to the cloud. However, making such an attempt brought about serious problems and risks that need to be resolved. There are many parties (such as specialized equipment that collects data from the patient, authentication equipment, doctors, patients, etc.) that must be trusted before end users can send their personal health data to a third party. A novel "in-the-cloud" service platform for storing, consuming, and capturing health-care data is being developed, implemented, validated, and distributed as part of the data capture and auto identification reference (DACAR) project.

2. Literature Survey

Hesham *et al*. [1] Baseband units were turned off to reduce power consumption in accordance with an analysis of the remote radio head to power-efficient baseband unit ratio and customer ratio. The form depends on the cloud server's processing capacity as well as the demands of the user rate. Resource allocation in the cloud radio access network system is difficult as a result of these two features. A dual restriction packing method will solve the energy problem. Results were assessed under various user loads while making bandwidth allocations based on baseband unit interference and processing time constraints for frames. This showed that the energy consumption in the data centers was significantly reduced while maintaining the overall system rate required.

Apat *et al*. [2] suggested using cloud collaboration and fog computing to create architecture for effective healthcare. By bringing resources closer to consumers latency-based application architecture can provide innovative solutions and options for low-latency and energy-efficient data processing. To minimize network costs for consumers, lower node-to-node latency, and balance the loads on network devices, adding services to the cluster requires integration. The hop count has been used to construct a fog computing environment. This study addressed issues related to service placement for a specific application of health monitoring in a fog computing environment. The two existing algorithms were compared to a novel dynamic cluster algorithm with latency knowledge and resource considerations. It has been determined that our approach is better than two other algorithms.

Thiam and Thiam [3] to reduce power consumption while maintaining QoS research was conducted to determine the best migration in a data center and virtual machine (VM) policy allocation. Use the CloudSim simulator to build a cloud environment. There is both a real-world and virtual computer interface available. They evaluate and compare our methods with other methods to see what improves VM placement and migration. According to the simulation results, methods for VM migration and routing use less energy and shorten simulation times. VM management methods are being attention in a variety of situations. The placement and migration of VM s are a multi-objective optimization issues. As a result, the effectiveness of a data center is highly dependent on the supply and location of virtual servers.

In addition to improve energy efficiency preventing the deterioration of service quality (QoS) and removing hotspots, an efficient VM allocation strategy will also reduce data center operating costs. It may be possible to increase cloud server utilization and lower cloud data energy consumption by moving VMs to fewer physical machines [19].

Moghaddam *et al*. [4], an energy-conscious VM selection strategy is implied by the analysis of the decline in migrations and SLAVs. The three steps of load balancing are as follows: Selecting destination hosts for chosen VMs after (a) Locating over-and- underused hosts and (b) choosing VMs to move from those hosts. The selection of the CPU load-balancing VM was the focus of the research. The CPU usage of VMs running on each host is taken into account by this suggested VM selection method, as well as any linear relationships between the CPU usage in VMs. Google and two different cloud data sets from the real CoMon project were used to test this technique. Its efficiency was evaluated in comparison to our benchmarking technique, which only considers VMs with the shortest movement times. We established that the ESV (SLAV × Energy Usage) and the number of "re-cover hosts" are highly correlated with the CPU usage of VMs in the data set by 64% and 81%, respectively. We also demonstrated that the SLAVs are 66% lower. (Like with the Google data set, for instance.) Costs associated with running a DC account for a sizable portion of energy use. As utility-based IT services and Cloud data centers have grown in size, the energy consumption of data centers has also increased significantly. For energy efficiency, Dynamic Cloud distributes their physical resources (e.g., hard disks, CPUs bandwidth, and RAM) on demand.

Puneetha and Nirmala [5] the decentralized Power-Aware Best Fit Priority algorithm which places VMs on hosts with the smallest increases in energy consumption. Uneven server use is identified using the concept of "skewness" and dynamic upper and lower limits for VM consolidation are set using the median absolute deviation policy. These techniques help us manage host overload and underload conditions as well. Data centers which have more software networks and remote sites are increasingly common due to the rise in popularity of cloud computing allow for centralized data storage and online access to resources and services. Cloud providers must manage demand growth, maximize energy efficiency and uphold strict performance standards despite the advantages of customers using less energy.

Vats *et al*. [6], due it is so cost-effective and simple to use cloud computing that is utilized everywhere. VM technology can be used by the cloud provider to effectively manage the resources due to sudden increase in demand for computer power. The methods of increased CPU usage and VM management that can reduce the energy consumption are examined in this study. Different cloud data centers exist, including ones with CPU, memory, and bandwidth. The CPU is regarded as the main resource in this technology because energy consumption is proportional to CPU utilization.

Fan *et al*. [18] developed a platform for collecting medical data to be processed through cloud computing. The authors did not address how to modify the platform for use with other architectures or how to develop services specifically for heterogeneous clouds where the platform is based on its architecture. As previously mentioned, administrators can implement and move an eHealth system to different cloud computing systems using a flexible and dynamic cloud platform.

Krishna *et al*. [17], the study has focused purely on wireless sensor networks and has only conducted a research on secure cloud architecture. The study excludes architectural elements like dynamic services and service modifications.

[20], the described architecture focuses on mobile user features and the entire architecture is not covered by the study. At FTaaS, we illustrated how the suggested platform implements a dynamic service.

[21] for cloud services that provide eHealth applications, a novel security model was proposed along with a list of security requirements. It focuses on the exchange of EHRs rather than developing, integrating, and deploying a broader range of eHealth services.

[23], after realizing the need for an e-consent language to record particular grantees, validity periods, purposes, operations, and a new language called e-CRL was proposed. In industries other than healthcare, such as law enforcement and social services, the DACAR policy syntax has been successfully implemented. It is just as functional as e-CRL.

Kilic *et al*. [22] described the peer-to-peer network used to exchange EHRs between various eHealth communities. A super-peer representing an eHealth community is in charge of routing messages and trying to alter the distribution meta data vocabularies that are used by various communities. While a single point of contact (SPoC) of the DACAR platform and this superpeer design is comparable, an SPoC offers more authorization functionalities.

Springall *et al*. [7], file transfer protocol (FTP) was used to address how the EHR is transferred to the network server FTP. Because security was not given much consideration when the traditional FTP protocol was being considered,

it has a well-known security limit. A secure FTP (FTPS) is used in the presented health-care system as a means of providing FTPS security solutions and approaches. This protocol protects FTP sessions.

Paladi *et al*. [15] for eHealth systems based on infrastructure-as-a-service (IaaS) clouds introduced a framework for protecting data confidentiality and integrity. Transparent storage isolation between IaaS clients is provided by the suggested solution, which is based on trusted computing principles. It also provides XML-based language frameworks for secure data sharing and defining access rights, which enables the lack of trustworthy data sharing mechanisms. The suggested changes were developed as a code extension for the well-known cloud platform Openstack. Despite becoming secure and having been integrated into an existing eHealth platform, the proposed framework lacks the flexibility of our design because patient data is stored in encrypted form across various domains. Although this method is viewed as a good practice that advantages from trusted computing principles, it specifically targets the IaaS model.

Yi *et al*. [11], an evaluation of the proposed architecture effectiveness was done on a prototype using Intel's Edison software. Three issues are addressed here: (1) Creating data sensing nodes for use in body sensor networks, (2) large amounts of data must be collected, stored, and analyzed, and (3) edge devices energy efficiency. With a service-oriented fog computing architecture, low power consumption, data reduction, and high efficiency were addressed.

[16] The issues of data compression, low power consumption, and high efficiency were addressed by the development of a service-oriented fog computing architecture. The overview provided by this is based on the use of a Swedish digital health-care record management system that is structured in the cloud. Moreover, this presented a new data integrity and confidentiality protection mechanism to provide a customer attack vector for cloud infrastructure. The majority of current methods take the difficulties of securely sharing patient data based on the set policies and access rights into consideration.

[24], the hierarchical model, application architecture, resource management mechanism framework for information system infrastructure for data backup, data management, and system monitoring were all described. Network traffic is decreased and system performance is increased even though security is not recognised.

Dubey *et al*. [12] diversified that environments are enhanced by the IoT-based health monitoring system that is being used. The design of the health-care system illustrates the value of service quality assurance, emergency notification, and bandwidth utilization.

[14] The efficacy of fog computing in health-care applications, a case research involved an electrocardiogram (ECG) is used. It implemented a variety of fog computing services including distributed databases, distributed user interfaces with access management, real-time notification systems, and location awareness. The Fog data are a generic architecture that allows a wide variety of wearable sensors such as smartwatch, wearable ECG system, and pulse glasses to be used for acquisition of health data.

Gia *et al*. [13], the resource management was evaluated. The relinquish probability methodology is proposed for resource management and estimation. There is no way to know how many resources will be used or whether all of the ones requested will be consumed. One can determine the appropriate amount of resources needed, which reduces resource waste and profits for fog.

[25] described a data mining model for helping physicians at the point of healthcare. For this model, neural network technology is used. The eHealth Cloud database serves as the knowledge base. The rules and the patient's data must be combined using an inference engine. The mining mechanism is built with the assistance of system-to-user communication. Artificial intelligence is based on neural networks, which are built using a lot of data. The neural network is composed of several layers, including output, input, and undefined hidden layers.

Lohr *et al*. [26] explains how medical data are transferred to mobile storage, which takes away security control from both the user end and the cloud. Making trusted privacy domains (TPD) is the plan of attack TPD. The TPD will evaluate all data transfers between the cloud and any other parties. Data will automatically be encrypted through TPD's secure gateway. TPD protects your data when stored in the cloud or anywhere else.

3. An Integrated Approach to Improve Dynamic Cloud Computing-based Health-care System Using DACAR

Figure 1 shows the block diagram of an integrated approach to improving a dynamic cloud computing-based health-care system using DACR.

The front-end (FTaaSeH) and the back-end (BTaaSeH) of this framework for eHealth systems are separate components. For standard services, FTaaSeH provides a generic and general interface. The uniform service interfaces of FTaaSeH are connected to specific cloud value-added services by BTaaSeH. Using the same FTaaSeH in a different cloud with a different BTaaSeH, this platform can easily be switched from one vendor's V1 to another's V2.

A dynamic layer called FTaaSeH enables cloud vendors to use it as a model for tailoring their cloud services. First, cloud vendors connect their value-added services through BTaaSeH to defined generic and uniform services using FTaaSeH. The uniform data access layer of a cloud service, however, provides a client with access to FTaaS through an abstraction (database access in this case).To access the platform's services, a client loads a web service called FTaaS Service Ref in this code. The client then makes a data access request using the web service's *GetDataList* procedure.

On the one hand, defined services in FTaaS can be customized by a cloud vendor to offer customers a range of services. An eHealth system can access services across heterogeneous cloud services to the BTaaS services that cloud vendors bind to their value-added cloud services.

An electronic medical record (EMR) that *FTaaS* has set up as a web service is requested by a client for data access. The client receives a general and consistent function from *FTaaS.* From *FTaaS,* the request will be forwarded to *BTaaS.* Data privacy method (DPM) and advanced encryption standard (AES) encryption are used as the two user-data protection techniques that are applied to each retrieved response. Windows communication foundation (WCF) implements *BTaaS* which is bound to a SQL database. At this level, they tested the performance of the suggested platform using a variety of queries and data protection techniques. The client at FTaaS receives BTaaS responses from a web service.

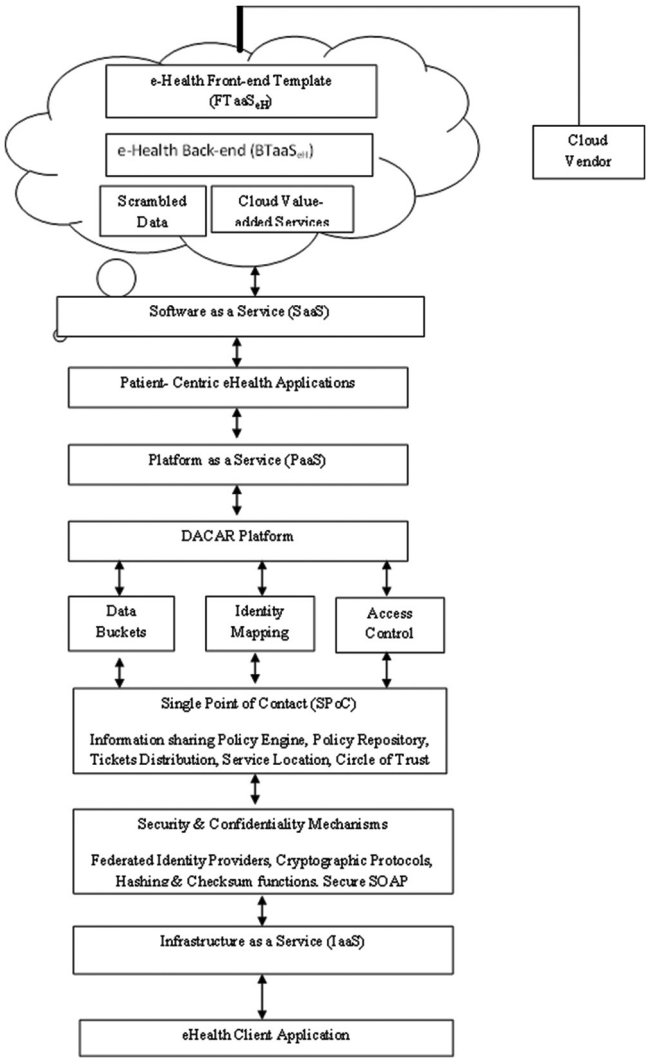

Figure 1: Block diagram of an integrated approach to improve dynamic cloud computing based healthcare system using DACR.

An *eHealth template* is part of the platform that has been put in place. Data access layer can be accessed from anywhere using the *FTaaS template*. *FTaaS* and BTaaS are implemented in the suggested platform as web services and WCF services, respectively. Traditional information technology systems or heterogeneous cloud computing systems can easily be integrated with *BTaaS* services.

However, with minimal client-side modification, an eHealth application and its data can be moved to another cloud provider. In addition, it can be expensive to modify the software for these devices and or sometimes necessitates hardware modifications, it is crucial to offer a generic and consistent service for mobile health-care devices.

Cloud computing service model known as "Software as a Service" (SaaS) allows vendors to offer a complete set of software applications to customers who subscribe to this "service" online. SaaS applications for healthcare replace traditional software while doing away with the need to own and host hardware. These applications include non-clinical information systems and clinical information systems (PACS, EHR, telehealth, etc). (billing, supply chain, etc). This type of cloud service does not require users to install or develop any applications. The underlying infrastructure is beyond the user control. They only use and customize the offered software services when necessary. SaaS advantages include cloud adaptability and significantly lower costs.

The patient-centric ehealth applications are the next step. Early warning score (EWS) a patient-centric ehealth application implemented on the DACAR platform is an example. EWS is a medical procedure that is commonly used in hospitals in the United Kingdom. The six vital signs of a patient must be routinely recorded and entered on a paper-based observation chart to use the traditional EWS. Staff members must also use predefined equations to calculate a patient's risk score. The medical staff should get in touch with the appropriate clinicians if a patient is considered to be "at risk". The manual nature of the measurement, recording, and calculation tasks makes the traditional EWS prone to errors.

In the new EWS application, vital signs are collected using radio frequency identification (RFID) sensors, the data are sent to data buckets monitored by smart handheld devices, and clinicians are alerted in real time through text or phones.

Developers never have to start from scratch when implementing eHealth applications or repeatedly deal with the same issues to platform as a service (PaaS) which offers a set of foundational services. Users can develop applications on the provider's platform. PaaS users do not need to install or maintain infrastructure to use the IaaS facilities. The CSP's platform tools are available for users to use (e.g., Server, Apache Server MySQL).

It utilizes a SPoC, rules-based policy syntax, and Cloud infrastructure built on scalability and affordability to securely collect, store, and consume sensitive health-care data. The DACAR platform is currently being developed into a prototype. Within a private Cloud infrastructure, an EWS demonstration was developed to test the platform's viability and performance.

DACAR's system model consists of the following concepts:

3.1. Domain

A distinct business area that is managed by a single organization is referred to as a domain. Multiple industries, including companies, pharmacies, insurance, hospitals, and research institutions may be involved in a health-care application. To create a circle of trust (CoT), the domains work together. Each CoT member maintains a list of reliable services provided by other CoT members.

3.2. User

A user is a person or a service that has been impersonated who uses an eHealth application. A user needs to be a part of at least one domain that can translate their identity into a particular role.

3.3. Object

An eHealth system's management of any entity including people and medical equipment is referred to as an object. A unique identifier (UID) given to an object by its owner domain serves as its identification. A content-oriented and contextual privacy attack should be able repelled by an eHealth system, meaning that even able to extract private information from storage or communication channels, the system should be able to withstand such an attack they should not be able to identify which data are linked to which object or establish a connection between the message's true source and destination. As a result, object UIDs should be substituted with opaque object pseudonyms.

3.4. Attribute

To describe an object, a set of attributes which are fundamental data types and atomic units of data is used. For instance, a patient object might have float-type attributes for blood pressure and heart rate along with a name attribute of the string type. Maintaining atomic attributes has two benefits. From atomic attributes, complex medical documents, like EHRs, can be generated dynamically. Second, while following fine-grained information sharing policies it is also possible to share atomic attributes between domains. In practice a variety of pertinent meta data including the location, capturer, unit device, and time that was used to collect the data must be stored in addition to the core value of an attribute. If sufficient meta data are preserved, eHealth applications can accurately reconstruct past medical events.

3.5. Service

As part of its SOA, DACAR integrates eHealth services for data capture, storage, and consumption. A service is a single instance of loosely coupled, message-based software with discoverable, coarse-grained that communicates with other services and applications. Many of the best practices from earlier software architectures, including autonomy, reusability, abstraction, loose coupling statelessness, and testability are incorporated into SOA.

Create, read, update, and delete (CRUD) operations and long-term attribute persistence are supported by Data Buckets, which collect, read, update, and delete attributes and meta data. Cloud buckets are associated with each attribute owner domain's SPoC and registered with CRUD services. Any application service cooperates with two conditions that can add data to or remove data from a data bucket.

The service first needs the target attribute's qualified name as defined by the domain ontology.

CRUD operations must be permitted on the attribute by establishing a rule authorizing the service or in the case of impersonation, the identity, or role of the invoker in the policy repository. If both conditions are met, the SPoC returns a Data Ticket with details about the CRUD endpoint, the permitted operations, the time limit, and a one-time session key encrypted using the CRUD service's public key and the requester's public key. In accordance with security policies, a Data Ticket may also contain instructions for data anonymization and sanitization that the CRUD service should follow.

User and object identifiers are resolved into pseudonyms by the identity mapping service and vice versa. Transparent user and object Ids should be replaced with opaque pseudonyms such as 12478*c*1*abd* in place of *PatientNo:*253, to improve the contextual privacy of an eHealth application. As a result, the DACAR platform only ever uses real identities to authenticate users for services and roles when it is absolutely necessary.

Patients can edit, delete, and delete create information sharing policies about their own characteristics using the access control service. The patient is viewed by DACAR as the true owner of their medical records and the organization takes a patient-centric approach. As a result, the patients should specify to their CoT who has access to such data. A user-friendly interface on the access control service makes it simple for authenticated users to set up rules that regulate who has access to personal information and what medical services they would like to subscribe.

To fulfill the authorization requirement, a SPoC is used. The domain ontology's operations, roles, definitions of object, attributes, services, identities, and access rights are stored in the policy repository. A CoT is made up of a network of peer-to-peer (P2P) SPoCs each of which represents a single domain (CoT). Through the P2P network, information requests are routed to SPoCs, which verify the requester's identity and role before granting access rights based on policy rules. As proof of an SPoC authorization, A *Service Ticket* or *Data Ticket* security tokens is protected and it is signed digitally by the SPoC.

Data integrity, confidentiality, and authentication requirements are met using security and confidentiality mechanisms. The more established RADIUS and Kerberos to the more recent OpenID and U-Prove user authentication protocols are all used by the various federated identity providers that DACAR collaborates with. Application developers can use the libraries and APIs provided by the DACAR platform to implement secure SOAP services. As a result, it is possible to subject the application-specific communication payload to a variety of security operations, such as digital signatures, hashing, and encryption integrity checksums.

A hybrid cloud infrastructure built on OpenNebular 2 and the Xen Hypervisor is known as infrastructure as a service (IaaS). For your health-care organization, these services will provide crucial technological resources, including data

processing, data storage, and the creation and deployment of ready-to-use applications among other things. The cloud hosts that make up the IaaS platform run VM guests and communicate with one another over a network. A PaaS provider that can host numerous external databases and is built on top of the IaaS platform is also assumed. A developer can create a searchable encryption-enabled eHealth application with the help of the API that the PaaS provider also offers and they can use it to evaluate the performance of the suggested platform.

EHealth client applications FTaaS access data from EMR implemented as web services. The client receives a generic and consistent function from FTaaS. The request will be sent from FTaaS to BTaaS. Both DPM and AES encryption are used to process each retrieved response to protect user data. WCF is responsible for implementing BTaaS and it is linked to a SQL database.

They ran different queries at this level, and use data protection methods to the EWS are a proof-of-concept application that has been constructed on top of the DACAR platform. In hospitals across the United Kingdom, EWS is a medical procedure that is frequently employed. Medical staff is required to regularly record and to calculate a patient's risk level, enter their six vital signs on a paper-based observation chart and use predefined equations. The appropriate clinicians should be contacted if a patient is evaluated to be "at risk" by the medical staff. Because all measurement, recording, and calculation tasks must be performed manually the traditional EWS is prone to errors. This procedure is completely automated by the new EWS application, which uses RFID sensors to collect vital signs intelligent handheld devices to transmit the values to data buckets continuously monitors patient status in real-time and notifies clinicians through phone calls or text messages.

Key generation algorithm

1. Keygen ()
2. Input: None
3. Output: public key rpk, secrete key risk, generator g,
4. {
5. The client runs random number generation in PaaS
6. A random number r is generated from the QR_N
7. Access e-health client application
8. }

4. Results Analysis

The result analysis of an integrated approach to improve dynamic cloud computing-based health-care system using DACAR is demonstrated in this section. The security has improved in this model. The query time also reduced in this design.

Table 1 describes the performance analysis of the presented an integrated approach to improve dynamic cloud computing-based health-care system using DACAR.

Table shows that an the performance analysis of the presented an integrated approach to improve dynamic cloud computing-based health-care system using DACAR gives high security, accuracy, precision, and less query time.

In Figure 2, security comparison graph the efficiency for an integrated approach to improve dynamic cloud computing-based health-care system using DACAR shows higher security when compared with other Figure 3 shows the Accuracy comparison graph

Table 1: Performance analysis

Performance analysis	Dynamic cloud computing based health-care system using DACAR	Dynamic cloud computing-based health-care system using AES
Security	98	91
Accuracy	98.4	92.7
Precision	97.8	89.9
Query time (ms)	0.7	1.6

AES: Advanced encryption standard

The graph shows higher accuracy when compared with dynamic cloud computing-based health-care system using AES.

In Figure 4, precision comparison graph the efficiency for an integrated approach to improve dynamic cloud computing-based health-care system using DACAR shows higher precision when compared with other models.

Therefore, in query time comparison graph as shown in Figure 5 shows less time for an integrated approach to improve dynamic cloud computing-based health-care system using DACAR when compared with the Dynamic Cloud Computing-based Health-care System Using AES.

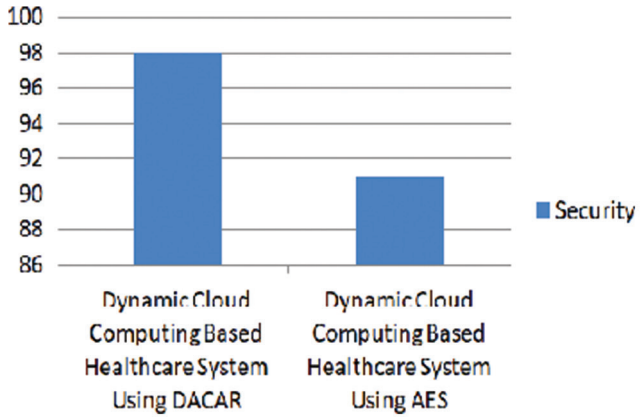

Figure 2: Security comparison graph.

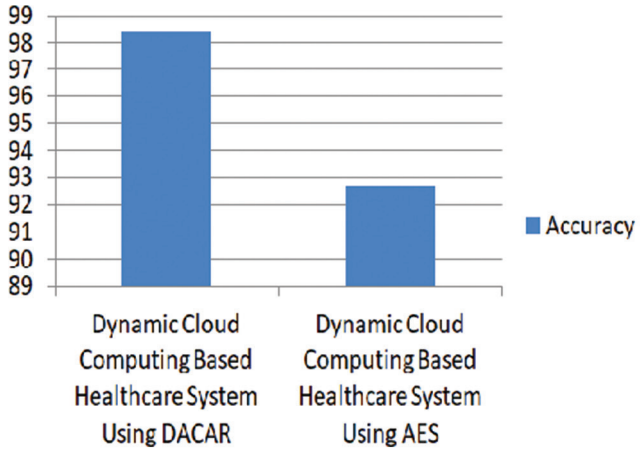

Figure 3: Accuracy comparison graph.

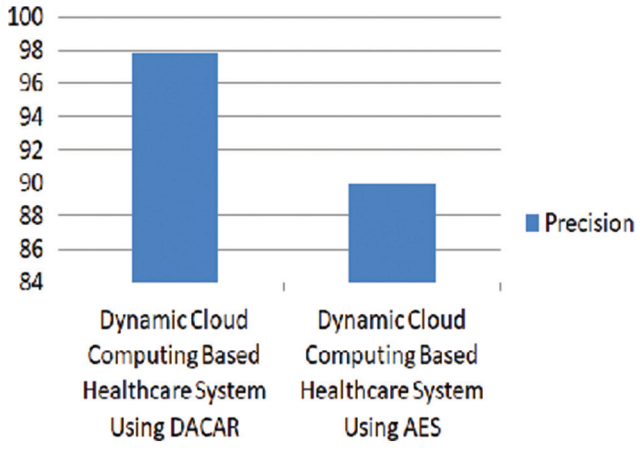

Figure 4: Precision comparison graph.

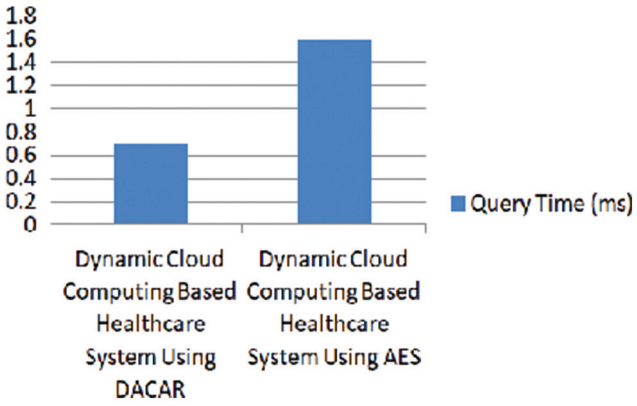

Figure 5: Query time comparison graph.

5. Conclusion

This paper presents a novel eHealth services platform designed by the DACAR project.The most fundamental requirements such as authorization, persistence confidentiality, authentication, audit trail, integrity, and secure data transmission the DACAR platform makes it easier to develop eHealth applications. Furthermore, it offers a variety of hardware and software options for combining the collection, storing, and utilization of private medical information. Third, it makes large-scale eHealth services deployable and deliverable through an efficient and reliable Cloud infrastructure. The design and implementation of these components, as well as the initial evaluation findings from the EWS demonstration application, are discussed in this paper. Because DACAR needs very little communication latency for application-level messages, it supports the creation and integration of time-critical eHealth applications. Cloud services provide scalable and reasonably priced buckets for hosting data and a SPOC to provide rule-based information sharing policies. Cloud infrastructure, sensitive health-care data could be collected, stored, and used securely.

6. Funding

"This research received no external funding".

7. Conflicts of Interest

"The authors declare no conflicts of interest."

References

[1] H. Hesham, M. Ashour, and T. El-Shabrawy, "An Energy Efficient Constraint RRH to Bbu Association in Cloud Radio Access Networks," In: *2020 37th National Radio Science Conference* (*NRSC*), IEEE, Cairo, Egypt, pp. 155-163, 2020.

[2] H. K. Apat, K. Bhaisare, B. Sahoo, and P. Maiti, "Energy Efficient Resource Management in Fog Computing Supported Medical Cyber-physical System," In: *2020 International Conference on Computer Science, Engineering and Applications* (*ICCSEA*), IEEE, Gunupur, India, pp. 1-6, 2020, doi: 10.1109/ICCSEA49143.2020.9132855

[3] C. Thiam, and F. Thiam, "An Energy-efficient VM Migrations Optimization in Cloud Data Centers," In: *2019 IEEE AFRICON*, IEEE, Ghana, pp. 1-5, 2019, doi: 10.1109/AFRICON46755.2019.9133776

[4] S. M. Moghaddam, S. F. Piraghaj, M. O'Sullivan, C. Walker, and C. Unsworth, "Energy-efficient and SLA-aware Virtual Machine Selection Algorithm for Dynamic Resource Allocation in Cloud Data Centers," In: *2018 IEEE/ACM 11th International Conference on Utility and Cloud Computing* (*UCC*), IEEE, Zurich, Switzerland, pp. 103-113, 2018. doi: 10.1109/UCC.2018.00019

[5] M. S. Puneetha, and M. B. Nirmala, "Energy Efficient Power Aware VM Scheduling in Decentralized Cloud," In: *2017 2nd International Conference On Emerging Computation and Information Technologies* (*ICECIT*), IEEE, Tumakuru, India, pp. 1-4, 2017, doi: 10.1109/ICECIT.2017.8453332

[6] S. Vats, S. K. Sharma, and S. Kumar, "Energy Efficient Resource Management in Cloud Environment: Progress and Challenges," In: *2016 4th International Conference on Parallel, Distributed and Grid Computing* (*PDGC*), IEEE, Waknaghat, India, pp. 636-641, 2016. doi: 10.1109/PDGC.2016.7913200

[7] D. Springall, Z. Durumeric, and J. A. Halderman, "FTP: The Forgotten Cloud," In: *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (*DSN*), IEEE, Toulouse, France, pp. 503-513, 2016, doi: 10.1109/DSN.2016.52

[8] M. Bahrami, and M. Singhal, "The Role of Cloud Computing Architecture in Big Data," In: W. Pedrycz and S. M. Chen (eds.), *Information Granularity, Big Data, and Computational Intelligence*, vol. 8, Ch. 13, Springer, Switzerland, 2015, pp. 275-295.

[9] M. Bahrami, and M. Singhal, "DCCSOA: A Dynamic Cloud Computing Service-Oriented Architecture," In: *IEEE International Conference on Information Reuse and Integration* (*IEEE IRI'15*), IEEE, San Francisco, CA, USA, Aug. 2015.

[10] N. Shu, and H. Jahankhani, "The Impact of the New European General Data Protection Regulation (GDPR) on the Information Governance Toolkit in Health and Social Care with Special Reference to Primary Care in England," in 2017 Cybersecurity and Cyberforensics Conference (CCC), IEEE, United States, pp. 31-37, 2017.

[11] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog Computing: Platform and Applications", In: *2015 3rd IEEE Workshop on Hot Topics in WebSystems and Technologies* (*HotWeb*)," IEEE, Washington, D.C., pp. 73-78, 2015, doi: 10.1109/HotWeb.2015.22

[12] H. Dubey, J. Yang, N. Constant, A. M. Amiri, Q. Yang, and K. Makodiya, "Fog Data: Enhancing Telehealth Big Data through Fog Computing," In: *Proceedings of the ASE Big Data and Social Informatics 2015*, IEEE, Kaohsiung, Taiwan, Oct. 2015.

[13] T. N. Gia, M. Jiang, A. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Fog Computing in Healthcare Internet of Things: A Case Study on ECG Feature Extraction," In: *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, IEEE, Liverpool, UK, pp. 356-363, 2015, doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.51

[14] S. Landau, "Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations," in: *IEEE Security and Privacy*, vol. 12, pp. 62-64, 2014, doi: 10.1109/MSP.2013.161

[15] N. Paladi, A. Michalas, and C. Gehrmann, "Domain Based Storage Protection with Secure Access Control for the Cloud," In: *Proceedings of the 2014 International Workshop on Security in Cloud Computing* (*ASIACCS*), ACM, New York, USA, 2014.

[16] A. Michalas, N. Paladi, and C. Gehrmann, "Security Aspects of E-health Systems Migration to the Cloud," In: *2014 IEEE 16th International Conference on E-Health Networking, Applications and Services* (*Healthcom*), IEEE, Natal, Brazil, pp. 212-218, Oct. 2014, doi: 10.13140/2.1.1616.7367

[17] T. Krishna, S. P. Praveen, S. Ahmed, and P. N. Srinivasu, "Software-driven Secure Framework for Mobile Healthcare Applications in IoMT," *Intelligent Decision Technologies*, vol. 17, pp. 1-14, 2022.

[18] L. Fan, W. J. Buchanan, C. Thummler, O. Lo, A. Khedim, O. Uthmani, A. Lawson, and D. Bell, "DACAR Platform for eHealth Services Cloud," In: *IEEE International Conference on Cloud Computing* (*CLOUD 2011*), IEEE, Washington, D.C, USA, 2011, doi: 10.1109/CLOUD.2011.31

[19] R. Zhang, and L. Liu, "Security Models and Requirements for Healthcare Application Clouds," In: *IEEE International Conference on Cloud Computing, CLOUD 2010*, IEEE, Miami, FL, USA, pp. 268-275, 2010, doi: 10.1109/CLOUD.2010.62

[20] S. P. Praveen, M. H. Ali, M. M. Jaber, D. Buddhi, C. Prakash, D. R. Rani, and T. Thirugnanam, "IOT-Enabled Healthcare Data Analysis in Virtual Hospital Systems Using Industry 4.0 Smart Manufacturing," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 37, p. 2350002, 2023, doi: 10.1142/S0218001423560025

[21] S. P. Praveen, T. B. M. Krishna, C. H. Anuradha, S. R. Mandalapu, P. Sarala, and S. Sindhura, "A Robust Framework for Handling Health Care Information Based on Machine Learning and Bigdata Engineering Techniques," *International Journal of Healthcare Management*, vol. 2022, pp. 1-18, 2022, doi: 10.1080/20479700.2022.2157071

[22] S. P. Praveen, T. B. M. Krishna, S. K. Chawla, and C. Anuradha, "Virtual Private Network Flow Detection in Wireless Sensor Networks Using Machine Learning Techniques," *International Journal of Sensors Wireless Communications and Control*, vol. 11, no. 7, pp. 716-724, 2021.

[23] L. Osman, O. Taiwo, A. Elashry, and A. E. Ezugwu, "Intelligent Edge Computing for IoT: Enhancing Security and Privacy," *Journal of Intelligent Systems and Internet of Things*, vol. 8, no, 1, pp. 55-65, 2023, doi: 10.54216/JISIoT.080105

[24] S. P. Praveen, H. Ghasempoor, N. Shahabi, and F. Izanloo, "A Hybrid Gravitational Emulation Local Search-based Algorithm for Task Scheduling in Cloud Computing," *Mathematical Problems in Engineering*,

vol. 2023, p. 6516482, 2023, doi: 10.1155/2023/6516482

[25] P. Sherubha, S. Sasirekha, A. D. K. Anguraj, J. V. Rani, R. Anitha, S. P. Praveen, and R. H. Krishnan, "An Efficient Unsupervised Learning Approach for Detecting an Anomaly in Cloud," *Computer Systems Science and Engineering*, vol. 45, no. 1, pp. 149-166, 2023, doi: 10.32604/csse.2023.024424

[26] S. P. Praveen, M. H. Ali, M. A. Jarwar, C. Prakash, R. K. R. Chavva, L. Malliga, and C. V. Chinnappan, "6G assisted federated learning for continuous monitoring in wireless sensor network using game theory," Wireless Networks, 2023, https://doi.org/10.1007/s11276-023-03249-0